



REPLY TO
ATTENTION OF:

DEPARTMENT OF THE ARMY
HEADQUARTERS, 25TH INFANTRY DIVISION
SCHOFIELD BARRACKS, HI 96857-6000

APVG-CG

5 November 2014

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: 25th Infantry Division Policy Letter 4 - Operations Security (OPSEC)
Standing Operating Procedures

1. References.

- a. National Security Decision Directive 298, National Operations Security Program, 22 January 1988.
- b. Department of Defense Directive 5205.02E, DoD Operations Security Program, June 20, 2012.
- c. DoD 5205.02-M, "DoD Operations Security Program Manual," November 3, 2008.
- d. AR 530-1, Operations Security (OPSEC), 19 April 2007.
- e. AR 380-49, Industrial Security Program, 15 April 1982.
- f. AR 381-12, Subversion and Espionage Directed Against the U.S. Army (SAEDA), 15 January 1993.
- g. AR 380-5, DA Information Security Program, 29 September 2000.
- h. AR 25-2, Information Assurance, 14 November 2003.
- i. AR 1-201, Army Inspection Program, 12 January 2004.
- j. AR 380-381, Special Access Programs (SAP), 21 April 2004.
- k. AR 25-1, Army Knowledge Management and Information Technology, 15 July 2005.
- l. AR 25-55, The Department of the Army Freedom of Information Act Program.
- m. AR 380-5, Department of the Army Information Security Program.

2. General. This administrative guide, henceforth known as a Standard Operating Procedure (SOP) provides instructions on how to effectively manage and oversee

Operations Security (OPSEC) within 25th ID. It establishes overall OPSEC standards and policies in compliance with all references listed above. This guidance applies to all 25th ID units and assigned military, civilian and contractor personnel.

3. Responsibilities.

a. 25th ID personnel will not publish or disseminate information without giving consideration to Information Assurance (IA) and OPSEC requirements. 25th ID personnel will support the mission, IA, and force protection by ensuring published information is correctly categorized, placed on the correct network and website, and protected properly with correct access controls.

b. 25th ID CIO/G6. Establishes policy to install, operate, and maintain all websites for 25th ID organizations. The 25th ID Headquarters Information Technology Support provides web server hardware and system administration for all organizations that publish publicly accessible information on the 25th ID Internet site and for the 25th ID HQ staff private sites.

c. Unit PAO. In coordination with 25th ID PAO, this individual is designated by the commander on duty appointment orders and reviews information for release to the unit's publicly accessible 25th ID Internet website. No information will be posted to a publicly accessible website without first obtaining a review and recommendation from the Unit PAO and approval from the organization's commander or civilian equivalent.

d. Data Owner (Originator/Proponent). The individual(s) who provide original content or information to a website. This individual is responsible for determining sensitivity of the document, determining the appropriate audience for the information and for gaining approval from their Public Affairs Office, OPSEC Officer, and Commander (or designated representative) before requesting publication of information. The proponent will periodically review content to ensure it is current and protected as necessary.

e. Content Manager. Normally at battalion level and higher, this individual manages all of the information created by an organization to ensure that it is authentic, current, accessible (to the authorized audience), preserved, and protected. The Content Manager coordinates with the data owner, commander, and Webmaster/Web Author to provide information to the intended audience.

f. Webmaster. The individual or group who administers the website hardware and software for units that are authorized to possess web servers (where server consolidation has not already occurred). Designs website layout and provides

appropriate encryption and access controls. Posts information in coordination with the data owner, Commander/Content Manager approval, and governing policy and regulations. Coordinates internal reviews of website information. Webmasters will have technical control over updating the site's content and will ensure the site conforms to Federal, DoD and Army-wide policies and conventions. Units that are authorized to possess web servers will not operate them without a qualified Webmaster.

g. Web Author. When server consolidation has occurred this is the individual who will coordinate with the server manager to post content to unit websites. Designs website layout and provides appropriate encryption and access controls. Posts information in coordination with the data owner, Commander/Content Manager approval, and governing policy and regulations. Coordinates internal reviews of website information.

h. Server Manager. When server consolidation has occurred, this is the organization/personnel that installs, operates, and maintains the web server hardware and software that units use to establish their web presence(s).

i. Commander. The final approval authority for all information published by the organization. The commander will determine the type of websites (Internet, Extranet, Intranet) necessary to publish information in support of his/her mission. The commander may delegate the final approval authority to publish information to the Content Manager.

j. Unit OPSEC Officer. Responsible for providing OPSEC reviews for content at the unit level during the web content approval process. Information will not be posted on any unit website (Internet, Intranet or Extranet) without OPSEC review and recommendation to approving authority. Coordinates additional OPSEC support as required through parent headquarters OPSEC Officer. OPSEC Program manager certification and training requests will be coordinated through the 25th ID OPSEC Program Manager. External OPSEC support may be requested from 1st Information Operations Command (1st IO Cmd.) or other agencies as appropriate. Conducts periodic web review of unit web pages ICW Unit PAO, Webmaster/Author, Content Manager and Data Owner(s).

4. OPSEC Implementation.

a. OPSEC is necessary for achievement of essential secrecy and surprise in United States (U.S.) military operations and activities. It is accomplished through protection of capabilities and intentions from hostile intelligence exploitation. Its ultimate objective is to prevent an enemy from obtaining sufficient advance information to predict outcomes,

and have the ability to degrade friendly operations or capabilities. Unless an adversary has access to planning actions by means of espionage that uses covert sources (e.g., agents, technical devices), they must often depend on unclassified information derived from detectable activities. Detectable activities include any emission or reflection of energy, any action or other indicator that can be easily observed or recorded, and all material available to the public via open source intelligence (OSINT). Both protected and unprotected information can frequently be obtained from detectable activities and indicators.

b. Mission accomplishment and effectiveness are relative to the adversary's capabilities and tactics used, and to the adversary's knowledge of U.S. intentions and military capabilities. The objective of OPSEC within 25th ID is to preserve the effectiveness of our capabilities and maintain the elements of initiative and security. 25th ID, command personnel, and tenant agencies will implement OPSEC measures to protect unclassified, operationally critical information while supporting or performing operational missions.

5. OPSEC Program Elements and Responsibilities. OPSEC must be an integral part of all military plans, operations, and activities. All units and their staffs must become involved in OPSEC planning. A sound appreciation of the adversary's capability to exploit OPSEC vulnerabilities is fundamental to proper OPSEC planning. Comprehensive OPSEC planning and incisive implementation ensures that the sensitivities of friendly operations are identified, vulnerabilities to the hostile intelligence threat are assessed, and protective measures are devised, evaluated, and executed. An effective OPSEC process is based on the development of sound program management with command emphasis. Strong OPSEC assessment, planning, training, and monitoring programs are critical components of mission effectiveness and an operational readiness posture.

a. Critical Sensitive Mission Areas. This should be identified by the OPSEC officer, with input from the OPSEC committee, of critically sensitive mission areas, which, if compromised, could jeopardize the organization's capability to perform its mission. This constitutes the Critical Information List (CIL).

b. OPSEC Assessments. This is performance of internal OPSEC assessments by the OPSEC officer, based on the command's mission and the identified or assumed hostile intelligence threat and the command's Essential Elements of Friendly Information (EEFI) and the Critical Information List. Additionally, the OPSEC officer will periodically request external assessments by the higher headquarters and other outside elements to gauge effectiveness of the 25th ID OPSEC program by a disinterested party. The 25th ID OPSEC Program Manager will conduct periodic inspections of work areas, trash handling procedures, and recycling efforts throughout 25th ID to enforce compliance with this policy.

c. Implemented measures. This is assurance by leaders that OPSEC measures are deliberately considered and used in critical mission areas requiring protection from hostile exploitation. Such measures will be included in the OPSEC annex to all applicable orders and plans.

d. OPSEC Training. The institution of command-wide OPSEC training by the OPSEC officer is vital. Education is a key factor. All military, DOD civilian, and contractor personnel must understand the nature of the hostile intelligence threat to their areas of responsibility, the OPSEC concept, and the relevance of OPSEC to their assigned duties. Command OPSEC training programs will be designed to foster a continuing appreciation of OPSEC application to command mission and organizational activities. An OPSEC brief will be given to all 25th ID incoming personnel and their families during in processing. OPSEC principles and practices will be integrated into individual and unit training program objectives. All 25th ID personnel will receive initial OPSEC Level I training upon reporting into their unit, and will renew their OPSEC Level I training annually thereafter. OPSEC Officers will be OPSEC Level II trained and will administer OPSEC Level I training to their unit personnel. Effective OPSEC training will be job-oriented and relevant to assigned duties.

e. OPSEC Committee. The commander implements an active OPSEC committee from 25th ID staff directorates, community agencies and Direct Reporting Units (DRU) OPSEC officers to participate as an OPSEC working group as directed in AR 530-1. The Inform and Influence Activities section, G7; is the office of primary responsibility (OPR) for this process.

f. OPSEC Process. This is a continuous process to identify, analyze and protect information for Essential Secrecy. Essential Secrecy is the condition achieved from the denial of critical information to adversaries. It is every individual's responsibility to apply this process to their daily mission, and every leader's responsibility to ensure there is command emphasis on the 5-steps of this process, which are:

- (1) Identify critical information.
- (2) Analyze threats.
- (3) Analyze vulnerabilities.
- (4) Assess risks.
- (5) Apply appropriate countermeasures (OPSEC).

6. Critical Information. The purpose of identifying critical information is to determine what information needs protection. The OPSEC framework identifies, analyzes and protects information for essential secrecy. Critical information consists of unclassified and classified elements of information that are particularly vulnerable to exploitation by adversaries. This information provides answers to key questions that our adversaries are likely to ask about our capabilities, plans, procedures, and intentions. Answers to these questions can enable our adversaries to develop actions to counter our efforts. These elements of information often appear harmless, commonplace, or unremarkable in and of themselves; but hostile intelligence organizations can combine bits of seemingly harmless information to form a complete picture of our capabilities and plans. The 25th ID Critical Information List (CIL) comprises information that is critical to the 25th ID mission. Personnel in the 25th ID—whether military, civilian, or contractor—will not discuss or transmit critical information on non-secure telephone or fax lines, through non-DOD or unencrypted NIPRNET e-mail, through publicly accessible Internet sites, or in public places where conversations can be overheard or electronically monitored, unless the information has been publicly released through proper channels. This includes commenting on or confirming details of critical information that has been improperly released to the public. CILs are “living documents” and are adapted to various operations and specific units. All 25th ID subordinate units are required to develop a CIL specific to their mission. These subordinate lists, however, must include all elements of the 25th ID CIL. The 25th ID Operations Security Manager will review the 25th ID CIL annually for continued currency and relevance to the 25th ID mission. The 25th ID CIL is also on the 25th ID Portal. A copy should be posted in all work areas, referred to in command briefings, and made easily accessible to all 25th ID personnel. Although the CIL is neither classified nor considered sensitive information, it should not be publicly distributed. Critical information must be protected to support operations security. Protecting and properly disposing of critical information is everyone’s responsibility.

7. Essential Elements of Friendly Information (EEFI). EEFI are critical aspects of a friendly operation that, if known by the enemy, would subsequently compromise, lead to failure of, or limit success of the operation and therefore, must be protected from enemy detection.

8. Operations Security Vulnerabilities. The 25th ID scope of operations, its location and its mission can create opportunities for intelligence collection by other nations and adversarial groups. There are a wide range of facilities, operations, activities and programs susceptible to penetration and/or exploitation by adversaries. Vulnerability exists when the adversary can observe an indicator, correctly analyze the information, make a decision and take timely action to degrade friendly operations.

9. Operations Security Measures. In deciding what protective measures are needed and their required duration, consider the time required for a collection system to obtain,

report, evaluate, and provide data to the adversary commander and the time at which effective adversary decision making will no longer be possible.

a. Much information and material about military operations and activities may not qualify for classification under the provisions of AR 380-5, but could be of substantial value to hostile intelligence services particularly when:

- (1) Aggregated over time.
- (2) Focused on a discrete activity or long-term project.

b. Such material if carelessly handled or disposed of would allow adversaries to:

- (1) Make more accurate estimates about related information that is classified.
- (2) Gain specific data that permits them to refine their EEFI menu.
- (3) Gain specific data that permits them to specifically target their more costly, sensitive, and scarce technical collection assets against CIL targets that cannot be obtained through easier and less resource-intensive, open-source collection methods.
- (4) Permit simplified accumulation of useful data (putting the puzzle together).

c. Examples of information that require protection regardless of their unclassified nature are technical manuals and drawings associated with classified hardware; reports of inspections that reveal vulnerabilities of an installation (other than those of an administrative nature); legal opinions, audits, investigations and surveys that pertain to safety, security, internal management, or operations of subordinate commands, etc.

d. When disposing of printed material that includes information from the 25th ID Critical Information List or information that is otherwise critical or sensitive, 25th ID personnel will shred the material by using an approved shredder. In short, the policy is to cross cut shred everything. This includes printed items such as work-related documents, personal items, and other documents with information that is critical to military operations, personnel security, or both. In support of this shred policy, all paper receptacles and trash bins will have a conspicuous notice using the words, "Shred Everything". Newspapers and magazines need not be shredded unless personnel have written critical or sensitive information on them. The intent of this policy is to reduce the possibility of accidentally disclosing critical or sensitive information. The standards in AR 25-55, paragraph 4-501, for destroying For Official Use Only (FOUO) information are insufficient to ensuring that critical and sensitive information generated or merely used by 25th ID is properly destroyed. Shredding, however, meets the requirement for destroying FOUO material, and solves the dilemma about what to do with materials

APVG-CG

SUBJECT: Policy Letter 4 - Operations Security (OPSEC) Standing Operating Procedures

marked as "Unclassified". Shredding is the most effective and practical means of destroying material in a way that prevents the possibility of its being reassembled. Shredding critical and sensitive material therefore supports OPSEC. All printed materials that are unclassified, classified FOUO, or of a higher classification must be cross-cut shredded using a shredder that is authorized by the Physical Security Officer to shred material of that level of classification or lower.

10. OPSEC OIC/NCOIC. In accordance with AR 530-1, the OPSEC OIC/NCOIC will at a minimum have at least one year of retainability in the unit, possess a Secret level clearance, and become OPSEC Level II certified within 30 days of appointment. Although not mandatory, OPSEC program managers may opt to receive OPSEC Level III Training which will certify them to conduct OPSEC Level II training. As directed by AR 530-1, the appropriate rank/grade level for OPSEC program managers and OPSEC officers are as follows:

- a. Division: Captain (O-3) or above, Warrant Officer (CW2 or above), Noncommissioned Officer (E-8 or above) or DA civilian equivalent.
- b. Brigade: Captain (O-3) or above, Warrant Officer, Noncommissioned Officer (E-7 or above) or DA civilian equivalent.
- c. Battalion: First Lieutenant (O-2) or above, Warrant Officer, Noncommissioned Officer (E-6 or above) or DA civilian equivalent.
- d. Below Battalion level: Any Officer, Warrant Officer, Noncommissioned officer (E-5 or above) or DA civilian equivalent as required.

11. Point of contact for this program is the 25th ID Inform and Influence Activities OPSEC Manager, DSN 655-6012.

Encl
as


CHARLES A. FLYNN
Major General, USA
Commanding

DISTRIBUTION:
A

25th ID Critical Information List

This list should be posted in all work areas, easily accessible, but out of public view. This list is also available on the 25th ID G3 webpage on the NIPRNET and the SIPRNET.

Know and protect critical information. The CG, 25th ID, considers the following as critical information:

☐ **Personnel Status and Personally Identifying Information.**

- Detailed information in casualty reports before next-of-kin notification.

NOTE: Generic information may be released by the public affairs office before next-of-kin notification.

☐ **Tasks and Support to Plans, Exercises, or Operations Involving U.S. Forces, Allies, and Partners.**

- Plans and operation orders for training exercises.
- Movement or deployment information for training exercises.
- Intelligence-support operations that are part of tasking orders, operational orders, or unit-movement orders.
- Serious incident reports.

☐ **Tactics, Techniques, and Procedures for Ongoing Operations Involving U.S. Forces.**

- Includes the use of or training on new equipment and new TTPs.

☐ **Readiness Status of U.S. and Allied Forces.**

- Operational readiness and support capabilities of U.S. or allied forces.
- Mobilization preparation.
- Unit operational readiness reports. According to AR 220-1, these reports are classified at least Confidential when aggregated at battalion level or above and for specific types of separate organizations.

☐ **Details of Issues between the U.S. Government and Its Allies and Partners.**

- Political communication between the United States and other nations that is not currently acknowledged or publicly known.

- ☐ **Current or Proposed Rules of Engagement and Rules on the Use of Force.**

- ☐ **Force, Communications, and Information-Protection Measures.**

- Current antiterrorism/force-protection measures, plans, and contingencies.

- Future or anticipated force-protection measures based on hostile or emerging threats.

- Scheduling and personnel rosters of unit and contractual security guards, command and control locations, and facilities for guard forces.

- Identification and location of key U.S. or allied mission command networks and systems and command relationships.

- Computer-user names and passwords.

- Details of network infrastructure.

- Details on information operations conditions and defense condition levels.

- Identification of critical infrastructures, communications nodes, and points of failure at U.S. or allied-nation facilities.

- ☐ **Details of Key Leader or VIP Movements.**

- Travel information concerning 25th ID key personnel.

- Identification, timelines, or locations of visiting VIPs.

Report any suspicious activity to the SSO at (808) 655-4121